

GDPR compliance



by



Day III
Class 3.
DPO Certification Part II
Bruxelles

Overview



abc

FAS

- Introduction to GDPR
- Changes
- Roadmap for implementation



DPO Day 1

- GDPR in practice
- Principles for data processing
- Legitimate interests and new rights
- Operational privacy



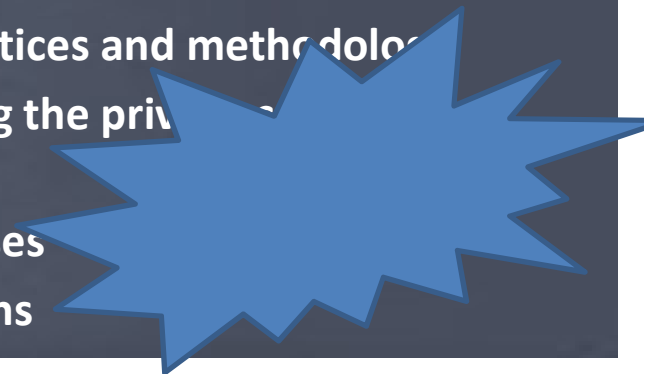
DPO Day 2

- DPO rule and functions
- Binding corporate rules
- Data protection impact assessment
- ISO 27001



CEP

- Best practices and methodology
- Managing the privacy program
- Study cases
- Definitions



Agenda

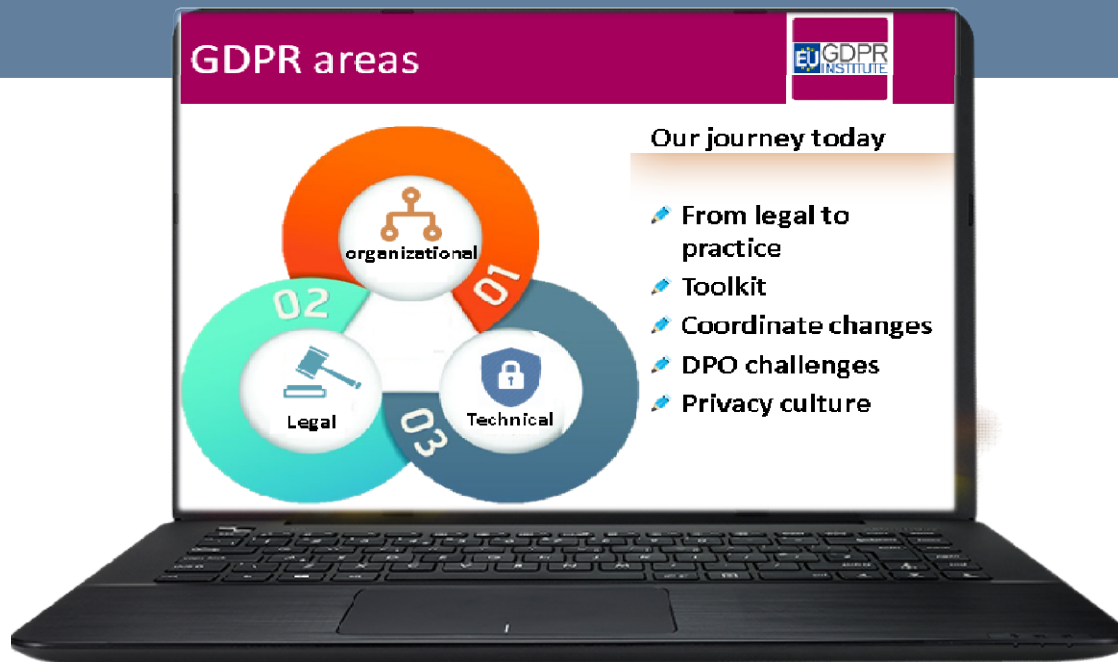


Time	Topic
09:00 - 09:25	Recap: Values of Data Protection & Privacy
09:25 - 10:30	Plan – DPO’s Role, Responsibility & Tasks
10:30 - 10:45	
10:45 - 11:05	Plan – Governance Plan
11:05 - 12:00	Plan – Binding Corporate Rules
12:00 - 12:30	
12:30 - 13:30	Do – DPO: Scenario Planning
13:30 - 14:20	Do – DPO: The six concluding steps
14:20 - 14:35	
14:35 - 15:35	Perform – Execute The DPO Role
15:35 - 16:30	Perform – DPO Exam

Access to the presentation



<https://www.eugdpr.institute/dpo-2/>

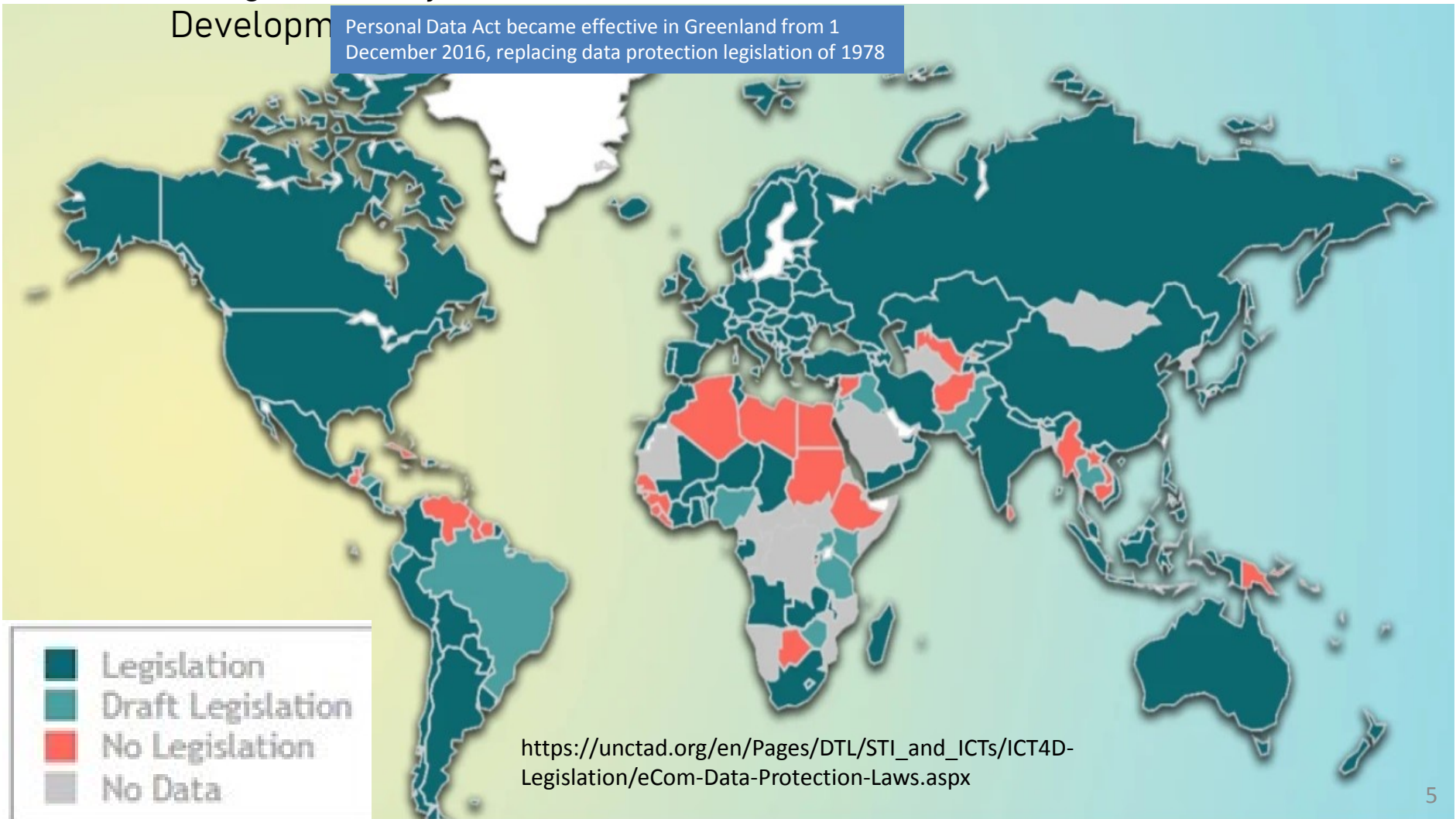


Global Data Protection and Privacy Legislation



[Image: courtesy of United Nations Conference on Trade and Development]

Personal Data Act became effective in Greenland from 1 December 2016, replacing data protection legislation of 1978



Current trends in the data protection industry



- Data management is continually being challenged—privacy, regulatory violation, legal impact, AI, cloud contracts
- Security vulnerability within the company processing and control infrastructure—authentication, authorization, access control, cryptography, encryption, monitoring
- The threat of “Monoculture” —diversity, resiliency, disaster recovery, business continuity and cyber security
- Data Processor/Service-Level Agreements—vendors and 3rd parties offer flexible, negotiated, customer-specific versions
- Heterogeneous big data and cloud computing environments—the ability to integrate with internal cloud and other (external) cloud vendors

Current trends in the data protection industry



- Technology is becoming smarter & more intuitive
- Legal issues need to be coupled with a people-centric design to engage and integrate processes and controls
- Create designs that help people understand and control the way services use their data and IT
 - ensure that designs build trust, transparency, controls
- Create user-interface design templates that reflect how people actually behave and interact online

Current trends in the data protection industry



- Organizations are looking to contain IT, Privacy and Cyber risks and improve efficiency and scalability of their IT and data infrastructure through the use of hardware-assisted Virtualization Technology to improve flexibility and robustness of their traditional software.
- Place information security initiatives into place, training to address the greatest challenge i.e. the lack of skilled information security resources.
- Cyber security, Privacy and Protection of personal data challenges in new technologies, services, such as social media, networking, virtualization, cloud computing,
- Privacy and data protection gains increased the focus of governments and regulators as they attempt to keep privacy regulations out in front of the potential risks associated with the new technologies.

Current trends in the data protection industry



- Identify data privacy compliance metrics/trends
- Ensure that data protection processes and procedures are being adhered to
- Implement the necessary management reviews
- Simulate incidents (e.g. data breach) to audit data security protocols
- Independent testing and quality assurance via internal or external audit service providers (ISAE 3204)
- Formalize non-compliance and remediation
- Escalate concerns and risks to senior management

Global Privacy principles



General best practices when collecting, storing, using and disclosing personal information

Represent the core around which data or privacy protection has evolved



Developed before the internet era and have been resilient enough to withstand the test of time

Why we need privacy principles?



📍 Provide a **common language** and **terms** to engage with all stakeholders

📍 Help set **expectations**, stipulate **requirements** and define **obligations**

📍 Harmonize **legal** and **governance** requirements



📍 Create a **structural understanding** of privacy

📍 Make data subjects aware of their **privacy rights**

📍 **Sensitive** entities that deal with transactions involving **personal data**

Privacy principles



Consent

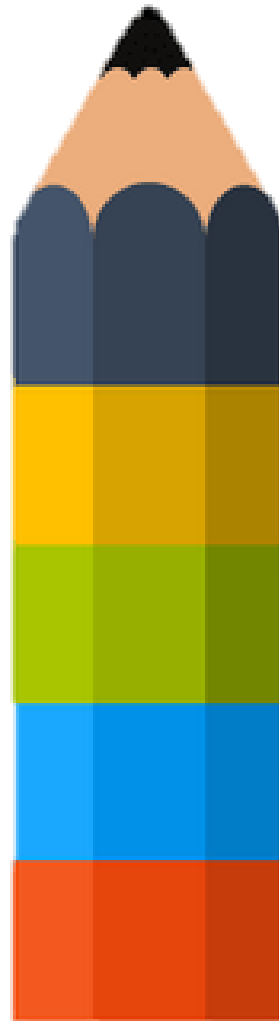
Data subjects understand and explicitly or implicitly agree with the uses of personal information

Notice

Data subjects receive a clear statement about the reason, the retention period, the access and the rights of personal information

Minimal use

Data controllers use personal information is only for a obtained consent



Choice

Data subjects make an informed decision regarding the permits on personal information

Minimal collection

Data controllers obtain personal information is only for a limited purpose

Privacy principles



Access and correction

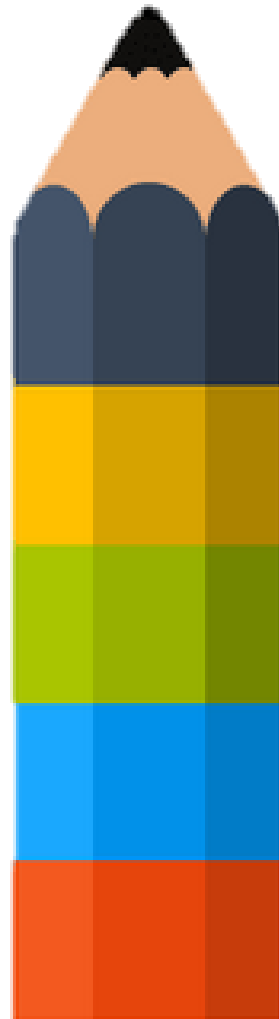
Data subjects access and correct personal information to ensure is accurate, complete and relevant

Security

Data controllers protect the access and modification of personal information

Transparency

Data controllers have understandable policies for data subjects and third parties



Accountability

Data controllers are responsible for complying this privacy regulations and principles

Disclosure

Data controllers can transfer and disclose personal information to third parties for the purposes described by the consents

New privacy principles



Privacy by design

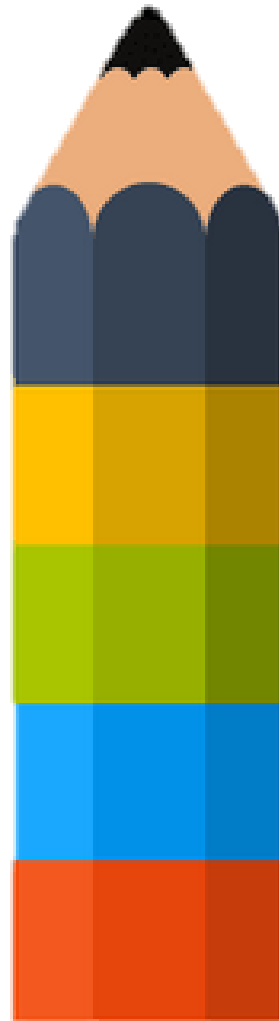
Data controllers consider privacy from the design to the complete development process of new products, processes or services

Anonymity

Data subjects have the option of not identify themselves

Right to be forgotten

Data subjects are allowed to erasure personal information from data controllers and third parties



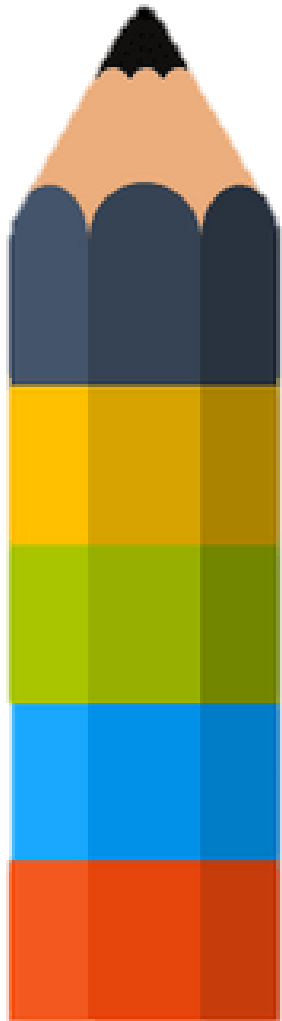
Sensitivity

Data subjects are more sensitive to personal information involving health, lifestyle and criminal records.

Enforcement

Data controllers should give assurance and certification on privacy policies and regulations

Privacy codes of practice



Organisational codes

Developed by a company or agency (generally public) to apply a privacy law (co-regulatory approach, should be approved by an authority)

i.e. Health Privacy Code of Practice

Sectorial codes

Developed by a trade association

i.e. Privacy code by the Federation of Direct Marketing

Functional codes

Developed to define privacy practices for a particular function

e.i. direct email and telemarketing

Professional codes

Developed by professional associations

i.e. Research for health

Technological codes

Developed by IT providers when a new technology arises

e.i. Walkie-Talkie privacy code



Global funds in the scope of GDPR?



- Global investment funds under any EU Financial Regulator will be considered data controllers regarding the EU investor data
- Service providers to the Investment funds will be regarded as data processors
- In certain circumstances, the service providers can also be considered as data controllers

How does GDPR effect non EU domiciled fund?



- GDPR applies to EU firms but also to firms established outside of the EU where the processing of personal data involves offering goods or services to EU ‘data subjects’
- Consequences depend on the carried out activities
- if a fund has European investors or is actively marketing to European investors it is in the GDPR scope
- If the Non-EU corporation is in the scope of the GDPR,
 - appoint a ‘EU representative’ to meet the obligations
- The EU representative will be the point of contact for any queries from the supervisory or oversight authorities or the data subjects about the fund’s activities

What do an non-EU domiciled company need to do?



- Draft and maintain a Data Protection Policy;
- Complete the data inventory to identify personal data processed by the fund and the lawful/legal basis for processing the data;
- Due diligence of data processors, e.g. the fund administrator;
- Training/awareness- informing and advising the board of their respective obligations under the GDPR;
- Act as the fund's EU representative where necessary.



DPO role and tasks



Please note that the data controller is responsible for GDPR compliance

- ✎ involvement in all issues relating to the protection of personal data of the data subject
- ✎ consult with controllers on DPIAs
- ✎ instruct controllers and processors on their obligations under the GDPR;
- ✎ receive communications from data subjects regarding their rights and processing of their data
- ✎ monitor compliance with the GDPR and related laws and the controller's policies
- ✎ facilitate or carry out audits; attend DP meetings, and cooperate and consult with supervisory authorities

The DPOs is independent



- ✎ DPO mandatory in organisations processing substantial volumes of personal data (article 37)
- ✎ A protected position, reporting directly to senior management
 - ✎ Appropriately qualified
 - ✎ Consulted in respect of all data processing activities
- ✎ Will be a ‘good practice’ appointment outside the mandatory appointments
- ✎ Most staff dealing with personal data (eg HR, marketing, etc) will need at least basic training
- ✎ Staff awareness training also critical (accidental release of personal data could have financially damaging consequences)

The DPOs is independent



- ✎ The DPO's independence as a center tent pole is holding up the whole canvas, and cannot lean in any direction
- ✎ DPOs have parallel responsibilities to the controller's operational teams, to the board of directors, to data subjects, and to the local oversight supervisory authority
- ✎ Controllers cannot instruct DPOs in the operation of their responsibilities but can provide the DPO with the necessary resources to carry out their duties
- ✎ Voluntarily appointing a DPO is encouraged by the EU's data protection authorities

The DPOs is independent



- ✎ The DPO is the “cornerstones of accountability,” facilitating GDPR compliance to create a potential competitive advantage for the business
- ✎ The DPOs cannot be penalized or dismissed by controllers or processors for performing their tasks
 - ✎ including termination of DPOs working under a services contract.
- ✎ Data subjects can initiate litigation against both controllers and processors for compliance breaches however data subjects cannot bring a claim against a DPO

Step 4: Compile a data inventory



What personal data do we hold?



Where is it?



What is it being used for?



How secure is it?

Data Landscaping: A value-based approach to document what data is held, why, for how long, where, where it came from, & with whom it will be shared, when and where.




Step 5: Discussion case



WIRED

Privacy

Wetherspoons just deleted its entire customer email database on purpose

-  **UK pub chain deleted their customer emails from marketing database in Jun 2017**
-  **Contacts are now by Twitter and Facebook**
-  **They suffered a breach of 665k emails in 2015**

Step 5: Discussion case



Dear Customer

I'm writing to inform you that we will no longer be sending our monthly customer newsletters by e-mail.

Many companies use e-mail to promote themselves, but we don't want to take this approach – which many consider intrusive.

Our database of customers' e-mail addresses, including yours, will be securely deleted.

In future, rather than e-mailing our newsletters, we will continue to release news stories on our website: jdaw@wetherspoon.com

You can also keep up to date by following our Facebook and Twitter pages, using the links below.

Thank you for your custom – and we hope to see you soon in a Wetherspoon pub.

Many thanks

John Hutson

Chief Executive

[Follow us](#)




[Like us](#)



Pros

 Less intrusive?

 No need to keep track of consents?

Cons

 Communication of offers

... but, by who?



Controller

Who decides
why the personal
data is needed

Processor

Who processes
the data

Service provider, cloud
services, outsourcing firms,
e-commerce platforms

Natural | legal person
including the government

... but, where?



in the EU

When personal data of individual living in the EU (citizens or not) is processed

outside the EU

When personal data of EU citizen is processed by a non-EU Organization **offering goods and services** in the EU (not paid in the EU)

Evaluating sub-processor risks



- Reviewing sub-processors risks could be complex by the implications of contracting with a non-EU software vendor
- Review the answers provided on a vendor questionnaire or the assurances of security commitments on encryption
 - Checklist on how an EU data processor/controller evaluate a non-EU sub-processor?
- Does the non-EU law provide clarification on individual privacy, communications, encryption...
- The consequences if the GDPR regime came into conflict with non-EU anti-encryption position, culture toward data privacy policies
- European organizations should identify third party, vendors headquartered or operating in non EU country & monitor local law(s)

Exercise



Case

Imagine that a ridesharing company (*i.e.* URBAN GO) based on a mobile app offers a platform where people (both drivers and riders) can register to use its service. The ridesharing company collects personal data of drivers and riders (name, address, driving license, bank account detail and location data etc.). The company has appointed a fintech solutions provider to process the payment (fare, driver's salary) and transferred all personal data to fintech company.

1. Identify the role – who is a data controller/data processor/data subject.
2. Based on your role, develop an outline of strategy to ensure data protection.

How personal data is processed?



Collect

Use

Destroy

Record

Transmit

Restrict



Change

Display



Electronically

Manually

GDPR covers personal information processed wholly or partly by automated means

Rights/Obligations under GDPR



Controller Obligations	Individual Rights
Clear Consent	Access to Data
Privacy by design & other considerations <ul style="list-style-type: none">– Lawful basis, fair processing, and specify purposes– Adequate, relevant, not excessive– Data accuracy, retention, and appropriate security	Remedy from supervisory body or court <ul style="list-style-type: none">– Compensation for damage– Compensation for distress Rectification
Clear, detailed Privacy notices	Objectification for direct marketing
Breach Notification	Erasure (Right to be forgotten)
Appointment of Data Protection Officer (high-risk processing)	Data Portability
International transfer adequacy	Restrict Data Processing (Put on Hold)
	Automated decisions and profiling

Extra-territorial application

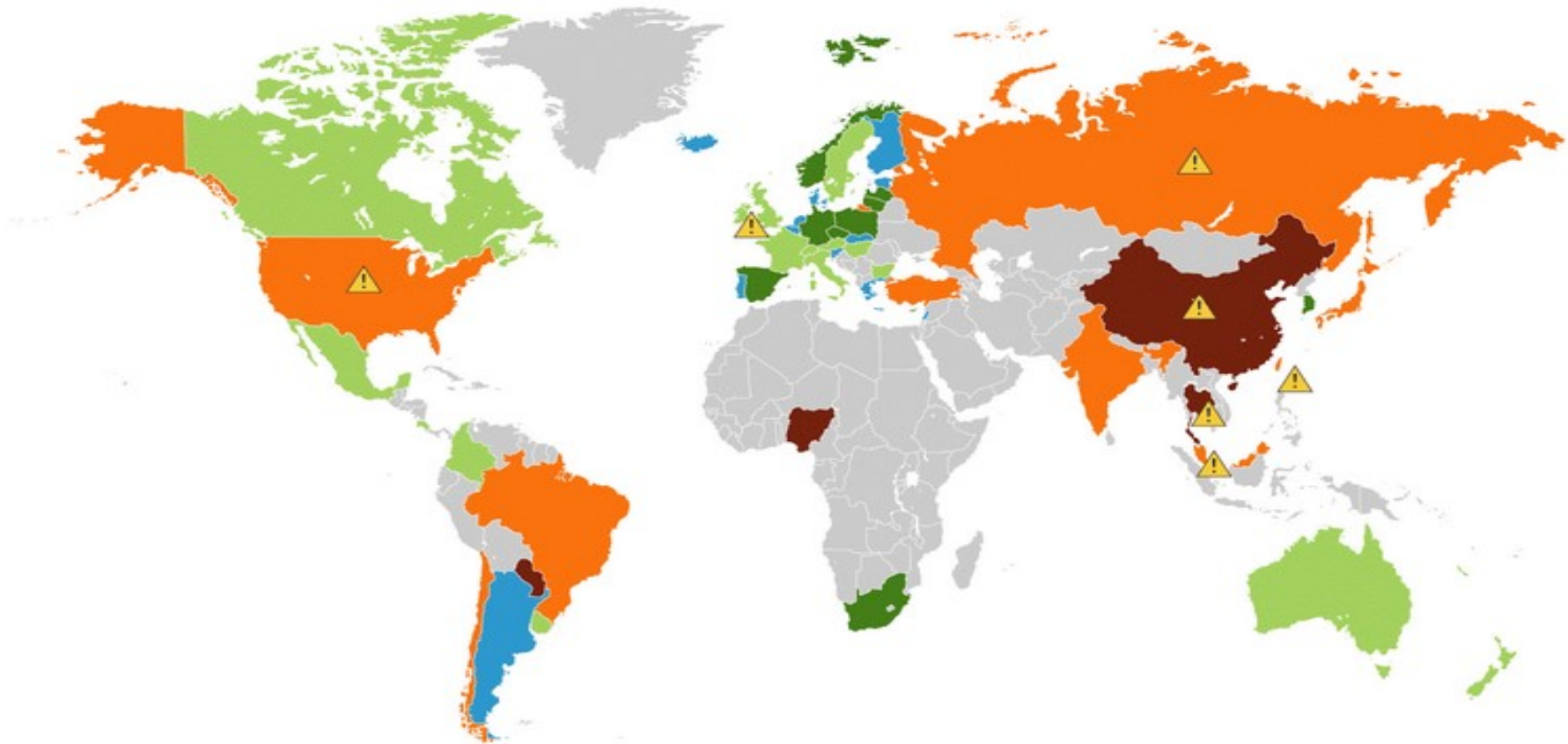


ACME
CORPORATION



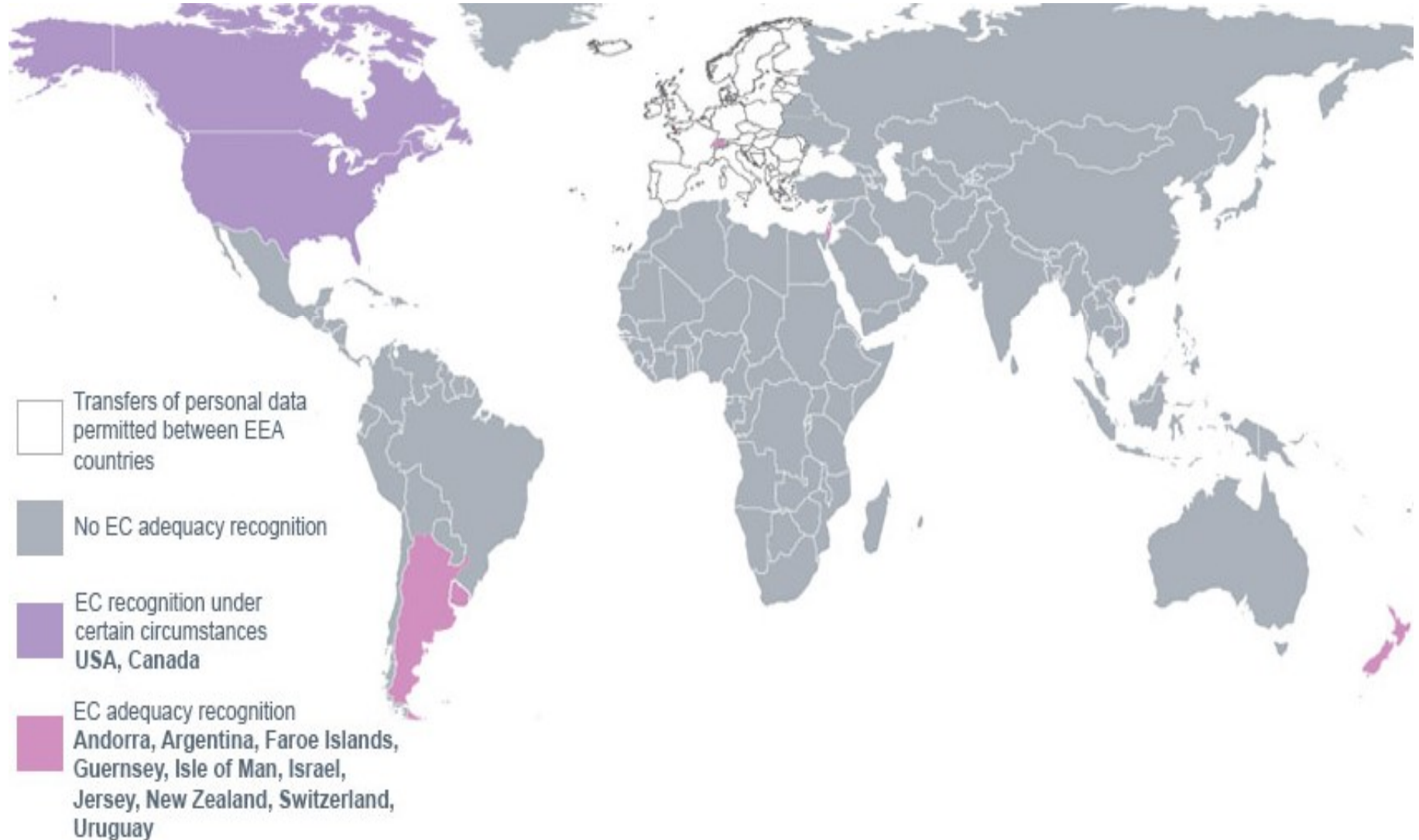
Ecommerce sites
targeting EU clients
(accessible from the EU, prices in
Euros, in EU languages, delivering
to EU)

Views on privacy



- Most restricted
- Restricted
- Some restrictions
- Minimal restrictions
- Effectively no restrictions
- No legislation or no information
- ⚠ Government surveillance may impact privacy

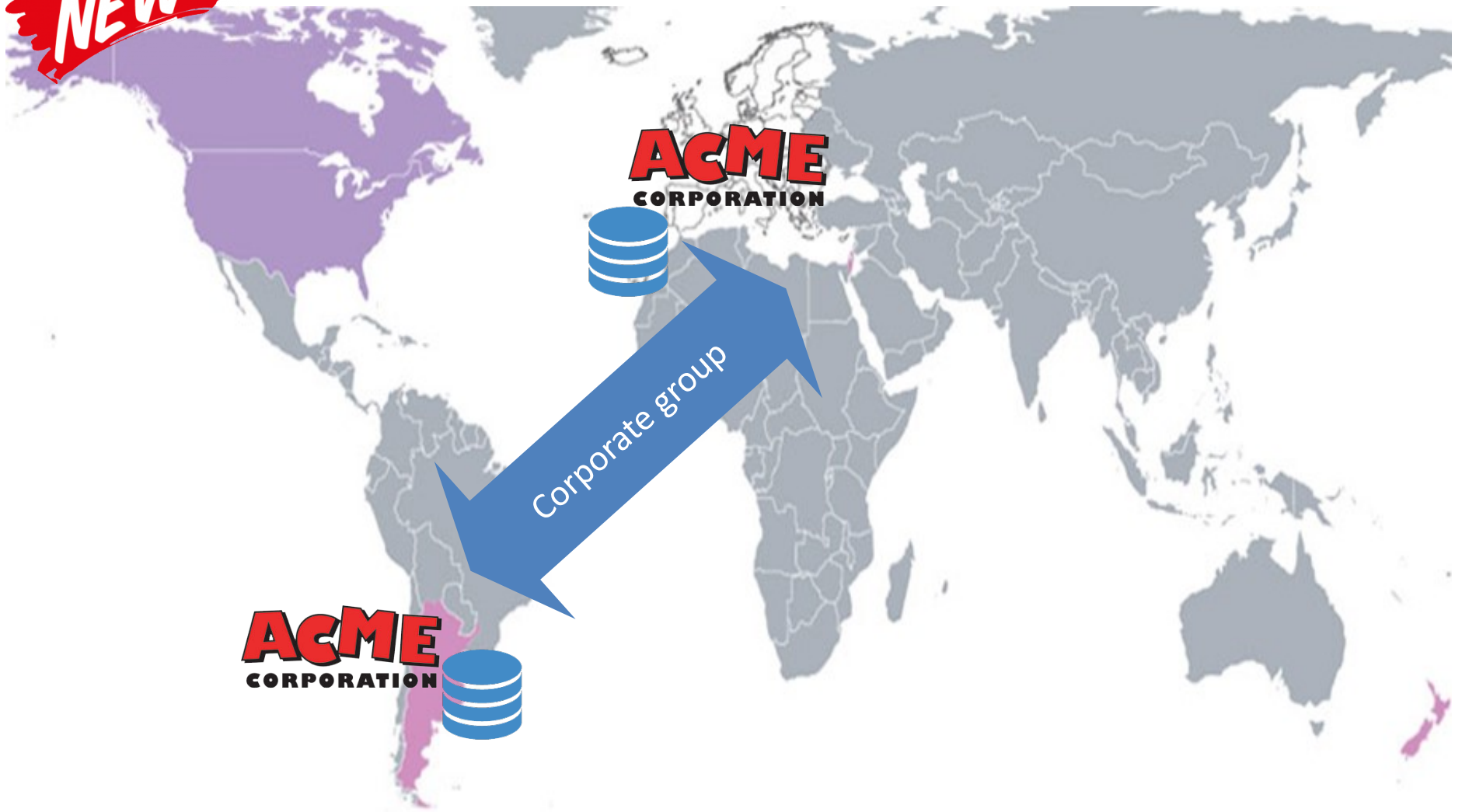
International transfers



Binding corporate rules



NEW



Binding corporate rules



Contract between group companies to transfer information, covering

- ✎ specify the purposes of the transfer and affected categories of data
- ✎ reflect the requirements of the GDPR
- ✎ confirm that the EU-based data exporters accept liability on behalf of the entire group
- ✎ explain complaint procedures
- ✎ provide mechanisms for ensuring compliance (e.g., audits)

Model pre-approved clauses to reduce compliance burden

Binding corporate rules



- ✎ BCRs allow companies to transfer personal data outside the bloc from a corporate group or a group of enterprises “engaged in a joint economic activity” operating within the EU to their components outside the EU
- ✎ The mechanism is primarily used by large companies, that have the resources to go through the exhaustive BCR approval process
- ✎ The GDPR, which takes effect in May 2018, recognizes BCRs as a legal means of transferring personal data from the EU

Binding corporate rules



Data Processors, Controllers

- ✎ The working party issued separate guidance for data controllers—companies that control the collection and use of personal data—and data processors—companies that process personal data under the instruction of controllers
- ✎ BCRs for processors apply to data received from an EU-based controller that isn't in the same corporate group and then processed by a member of the group
- ✎ BCRs for controllers apply to data transfers from EU-based controllers to non-EU controllers or processors within the same corporate group

Binding corporate rules



Data controllers and processors must now include

- ✎ The scope of the corporate group, including categories of data and types of processing; enforceable rights of individuals, including the right to lodge complaints; and demonstrated accountability

Data Processors must also include

- ✎ Privacy principles related to individual rights; and
- ✎ Service agreements containing all elements required by the GDPR.

Binding corporate rules



Controllers must also include

- ✎ Information on individual transparency rights related to processing of their data and the means of exercising those rights
- ✎ An explanation of privacy principles, including lawfulness, data minimization, storage limitation, guarantees of processing sensitive data, and onward transfer requirements to bodies not bound by BCRs;
- ✎ A list of any third-country legal commitments having adverse affect on BCRs will be reported to authorities.

Binding Corporate Rules



The GDPR expressly recognizes BCRs for controllers and processors as a means of legitimizing intra-group international data transfers

The BCRs must be legally binding and apply to and be enforced by every member of the group of undertakings/enterprises engaged in a joint economic activity, including their employees

BCRs must expressly confer enforceable rights on data subjects. The approach will be more streamlined with a clear list of requirements. This method of compliance is seen by some as the “gold standard” and is likely to become increasingly popular for intra-group transfers

Storage limitation	Deleting individual personal data records in databases, hadoop, and cloud storage	Fast erasure of individual records
---------------------------	---	------------------------------------

Standard data processor clause



The controller or processor can use standard data-protection clauses adopted by the Commission or by a supervisory authority

- Standard data-protection clauses between the processor and another processor
- To avoid any prejudgment of the fundamental rights or freedoms of the data subjects, controllers and processors
- Encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses
- Regulators have new rights to audit your compliance for businesses that operate in sectors where complaints to the regulators are frequent
- Identification of 'high risk' areas in processor contracts
 - creating a 'processor inventory' and identifying the high risk issues in the contracts based on, e.g. volume of personal data processed, where it might be accessed from and by how many sub-contractors/people, and how sensitive the data is.

Privacy Shield



- The premise of GDPR is the ‘harmonization’ of data protection laws across EU
- The U.S.-EU Safe Harbor, then the EU-U.S. Privacy Shield, and later U.K. Privacy Shield Shouldn’t other countries be subject to the same security with respect to compliance with EU data protections laws, with major countries like China, India and Russia.
- Five-step checklist:
 1. Develop and maintain a privacy policy based on Privacy Shield principles.
 2. Validate security safeguards with a customized security questionnaire deployed to system, application and interface owners who handle data that are subject to the certification.
 3. Address onward transfers by review and revising existing contracts for third-party vendors and other onward transferees.
 4. Update training for employees who have access to EU citizen data.
 5. Compile within a single compliance binder documentation that supports the company’s Privacy Shield certification—such as policies, a gap assessment report, and contract addendums.
- If firms wish to transfer HR data, they will have to indicate that separately in their self-certification submission and include details, such as their HR privacy policy.
- <https://www.bbb.org/EU-privacy-shield/privacy-shield-principles/>

Standard Contractual Clause



- The Article 29 Working Party provides a working draft on standard contractual clauses for the transfer of personal data from an EU data processor to a non-EU data sub-processor.
- Standard contractual clauses for the transfer of personal data to processors in third countries from an EU data processor to a non-EU data sub-processor.
- The working document amends or supplements existing model clauses currently in place under the Data Protection Directive.
- <https://ec.europa.eu/newsroom/article29/news-overview.cfm>

Standard Model Clauses



- The SMC incorporate information security requirements and sub-contracting liability concerns by striking a balance between company concerns and the rights of data subjects.
- if data processors decide to make modifications to previously agreed data processing contracts or decide to sub-contract the processing operations, then the amended contracts will need to comply with the model clauses
- Apply technical and organisational security measures in third countries.
- The measures should take into account existing data protection laws and balance the costs to companies in order to protect privacy data with adequate security precautions.

standard model clauses



- The data processor are liable for violations by sub-processors.
- The model clauses cover sub-processing to ensure
 - if the data processor subcontracts processing, such subcontractors will ensure that the personal data is protected (Clause 11).
- Complemented by third-party beneficiary rights granted to the data subjects to allow for their individual enforcement of the contract (Clause 3).
- This focus on individual rights is expanded by the data subject's rights to make claims and pursue compensation from the data controller for any breach by the data processor or sub-processors of its obligations in case of bankruptcy or insolvency proceedings concerning the exporter (Clause 6).

Example I



- What happens if a non-EU based vendor renders data hosting services on behalf of a corporation located in the U.S., and the data set comprises a large collection of personal data, mostly related to EU data subjects?
- The key issue is around Article 3, Section 2 of the GDPR in relation to the question of whether services are offered to individuals in the EU.
- The scenario described above has nothing to do with targeting EU people from the inception by offering services in order to boost sales.
- Hence, the GDPR does not apply.

Example II



- The non-EU company (Company A, the processor) offers data hosting services to another company (Company B, the controller).
- At face value, this scenario would not need to be GDPR compliant.
- However, if Company B (the controller) also acts on behalf of other legal entities within a group, and if personal data is transferred from these group legal entities to Company A (the processor),
- The arrangement may be caught by the GDPR.
- If one such group legal entity has an establishment in the EU, the GDPR comes into play via Article 3, Section 1.
- Therefore, all companies should closely review their service contracts from the perspective of group member involvement.
- A non-EU company can be under GDPR by entering into a service agreement based on this example

How do extra-territorial provisions apply to processors?



- A non-EU company is offering a consumer cloud service in the EU would clearly be affected by the GDPR (Article 3, Section 2).
- However, the overseas processor is only acting on the instructions of a controller, so would not be dealing with individuals in the EU of its own option.
- This circumstance does not shield it from the GDPR in general.
- The processor might still be caught where it is a sub-processor of a principal processor based in the EU.
- This is because the processor is processing personal data *in the context of the activities of* a controller or processor in the EU.
- Any provision of services to an entity in the EU might bring the overseas processor within the scope of the GDPR and in this instance the overseas processor(s) must be GDPR compliance

Step 5: How detect a data breach?



Indication of compromise

- ✎ notification from public authorities
 - ✎ FBI knocks at the door
- ✎ from users
 - ✎ oops, I opened a “funny attached file”
- ✎ alerts from 3rd parties
 - ✎ hosting vendor informed they had a malware
- ✎ continuous monitoring solutions
 - ✎ this server is transferring out a lot of amount of data

Incident response protocol

- ✎ Investigate “when” the breach was done
- ✎ Get the investigation team
- ✎ Investigate the level of compromise

Step 5: Scenario planning



Before the breach

- ✎ **Address IT risks and vulnerabilities**
 - ✎ all potential threats are identified and defensible (e.g. penetration testing, vulnerability scanning)
 - ✎ multi-layer cyber security defenses
- ✎ **Plan scenarios for responses**
- ✎ **Improve breach detection**
- ✎ **Require patches on DNS servers**

After the breach

- ✎ **Plan actions to contain damage**
 - ✎ business continuity, disaster recovery and reputation management (e.g. company crisis protocols)
- ✎ **Resilience! Plan how to move on from the breach**
 - ✎ Minimize the risk of future occurrence
 - ✎ Feedback from the incident response teams and affected people
 - ✎ Enhance and modify information security policies and training programs

Step 5: Scenario planning



Data breach response procedure

- ✎ Specific response requirements
 - ✎ Linked to the privacy risk assessments and data inventory
- ✎ Incident handling procedure
 - ✎ Clear accountability, communication, teams, external help
 - ✎ Scenarios } internal or external disclosure
malicious attack or accidental
- ✎ GDPR notification requirements
- ✎ Training to the response team
- ✎ Regular reviews and simulations (“real-life” exercises)

Monitor data leakage and loss

- ✎ Intrusion detection systems, firewalls, anti-virus/malware tools
- ✎ Threat intelligence
- ✎ Tracking of access and movement of personal information within the systems
- ✎ Network scanning for policy violations
- ✎ Log examination

Step 5: Scenario planning



Responding procedure

- ✎ Validate the breach
- ✎ Assign an incident manager (usually CISO) to investigate
- ✎ Assemble incident response team (IT, legal, public affairs)
- ✎ If breach is active, block accesses to systems and data
- ✎ Identify affected data, machines and devices
 - ✎ Full extent of the data compromised
- ✎ Preserve the evidence (logs, backups, images, hardware)

Monitor data leakage and loss

- ✎ Notification to data subjects fostering a cooperative help
 - ✎ If breach likely to result in a high risk to their rights (e.g. fraud, phishing, impersonation for credit application, credit card fraud, loss of reputation, discrimination), no need if breached data is encrypted
 - ✎ Scenarios: customers, employees, vendors
- ✎ Report to the Supervisory Authority
 - ✎ DPO role in 72 hours after becoming aware of the breach
 - ✎ Scenarios: inappropriate alteration or data loss
- ✎ Report to law enforcement in criminal suspicious breaches

Step 5: Discussion case



They even sell data breach services

- ✎ Equifax, main credit reporting agency
- ✎ Hackers exploited a security vulnerability in a US-based application
- ✎ Exposed names, social security numbers, birth dates, addresses of 143M US consumers and 200K credit card numbers!
- ✎ Required customers to froze their credit files, offered free credit monitoring and paid new credit cards
- ✎ Equifax had problems with data security before
- ✎ 41 days between discovery and disclosure
- ✎ Significant internal failure to communicate
- ✎ Executives sold 2M in shares just before disclosing
- ✎ Future class action suits

How can we manage the need to investigate a breach with the 72 hours rules to disclose a breach under GDPR?

Step 5: Discussion case



Popular restaurant app Zomato says the records of about 17 million users have been stolen in a security breach.

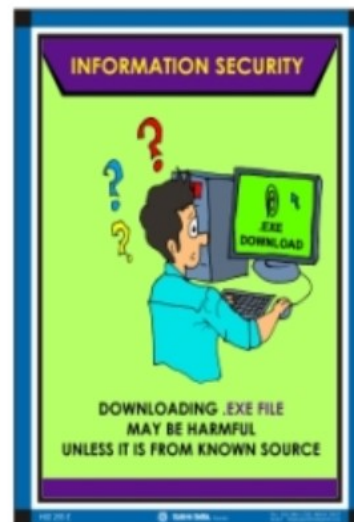
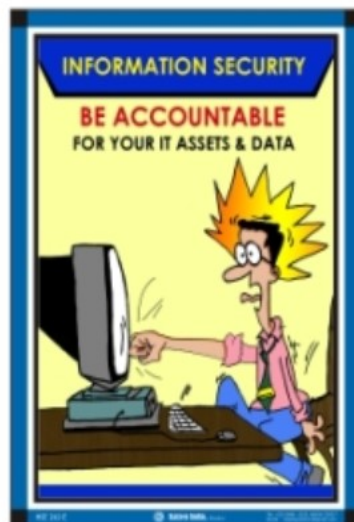
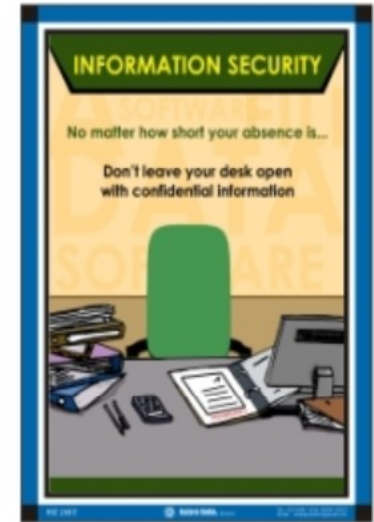
The Indian startup, which covers more than one million eateries across 24 countries, [said Thursday](#) that names, email addresses and encrypted passwords were taken from its database.

The company, which competes with Yelp ([YELP](#)), reassured affected customers that no payment information or credit card details were stolen.

Zomato said the security measures it uses ensure the stolen passwords can't be converted back into normal text, but it still urged users who use the same password on other services to change them. It also logged the affected users out of the app and reset their passwords.

"So far, it looks like an internal (human) security breach - some employee's development account got compromised," the company said in [a blog post](#), without providing further details. It didn't immediately respond to a request for more information.

Step 1: Train your people



Step 1: Discussion case



Data and Cyber Breach

- ✎ How could you develop training for this risk?
- ✎ How could you document your training efforts?



Let`s play... add controls to risks



Over collection of personal data

-  Assign a data owner, inventory

Incorrect or outdated personal data

-  Validation campaigns, data audits, interface controls

Unauthorized use or export by users

-  Minimum access, training

Unauthorized use or export by third parties

-  Liability clauses, security requirements

Let`s play... add controls to risks



- ✎ Missing consents / data subjects unaware of uses
 - ✔ Compulsory consent notices, process review
- ✎ Data subject cannot access or rectify their info
 - ✔ Protocol for requests, forms on line
- ✎ Fragmented systems cannot retrieve or update all the data
 - ✔ Updated inventory
- ✎ Personal data is hacked
 - ✔ Network activity monitoring, firewall
- ✎ Personal data is kept longer than intended
 - ✔ Automated deletion processes when data is flagged for deletion

1 – Identify the need



Early before **new** projects or revision of existing processes

for example, when considering a

- ✎ New system to store personal data
- ✎ Change the use of already collected personal data
- ✎ New video surveillance system
- ✎ Vulnerable data subjects (e.g. children)
- ✎ New database consolidating tables with personal information from other systems
- ✎ New algorithm to profile a particular type of client
- ✎ Proposal to share personal data with a business partner
- ✎ Impact of a new legislation

Existing processes → Recommended initial assessment

Doubts if needed → consult the Supervisory Authority and beg for mercy!

2 – Identify the flows



Process map start from the process or project documentation



Identify personal information in the process map



Consult with experts how personal information is collected, transferred, used and stored

 for existing and future purposes

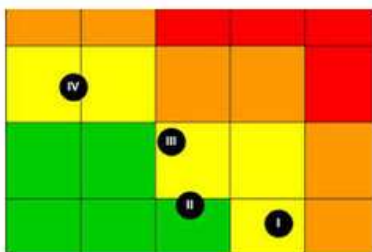
3- Consult on risks and controls



Consult all involved parties to have a 360° view, link risks to owners



Include current controls in the process map



Assess the impact and frequency in a heat map (recommended), risk assessment in ISO 27001 (under 29100)

- Impact: fines, business continuity costs, loss of clients, reputational damage
- Risk must be assessed from the view of the data subject, not the business!

4 - Identify new measures



Prioritize according to a tolerance to privacy risks, link to data classification policy, risks can be accepted



Devise solutions such as new controls and technologies according to the cost/benefit for the risk



Create an action plan and sign off the document by the manager in charge of type of information involved

Step 5: Audit compliance



- ✎ Ensure that data protection processes and procedures are being adhered to
- ✎ Implement the management reviews
- ✎ Simulate incidents (e.g. data breach) to audit protocols
- ✎ Independent testing and quality assurance
- ✎ Formalize non-compliance and remediation
- ✎ Escalate concerns and risks
- ✎ Identify compliance metrics and trends

Step 5: Audit compliance



Process	KPI example
Training	% of staff (or hours) trained on privacy policies (participated/passed, type of program, levels)
Incident	# of privacy incidents (by system, location, repeated or new) # reported data breaches
Audits	# non conformities # action plans on-going (and past due)
Consents	% consents obtained
Access control	% of credential validated
Compliance	# requests # complains # new projects with DPIA

6 – Follow-up



Communicate to stakeholders, bottom-up and top-down



Advance with action plans and document implementation measures (IT and non-IT changes)












Regular post-implementation reviews to assess if risks are mitigated and to ensure that solutions identified have been adopted. Re-assess the DPIAs at least every 3 years

People to consult



Internal


-  Data protection officer (usually leading the DPIA)
-  Project management leaders and developers
-  CIO, CISO and other IT experts
-  Compliance officer
-  Legal department
-  Internal audit executive
-  Risk management officer
-  Future or current users
-  Senior managers

External

-  Potential data processors and vendors
-  Experts

Group discussion



 **How would you link the dataflow map with the cross-border transfers?**



Data Protection Officer



One man army?



Implementation team <> Maintenance team

Define clear objective and responsibilities

Be a leader

Experience in project management, security, training and legal

Commit time to process subject experts

Document all the project activities

Who needs a DPO?



The controller

AND

The processor

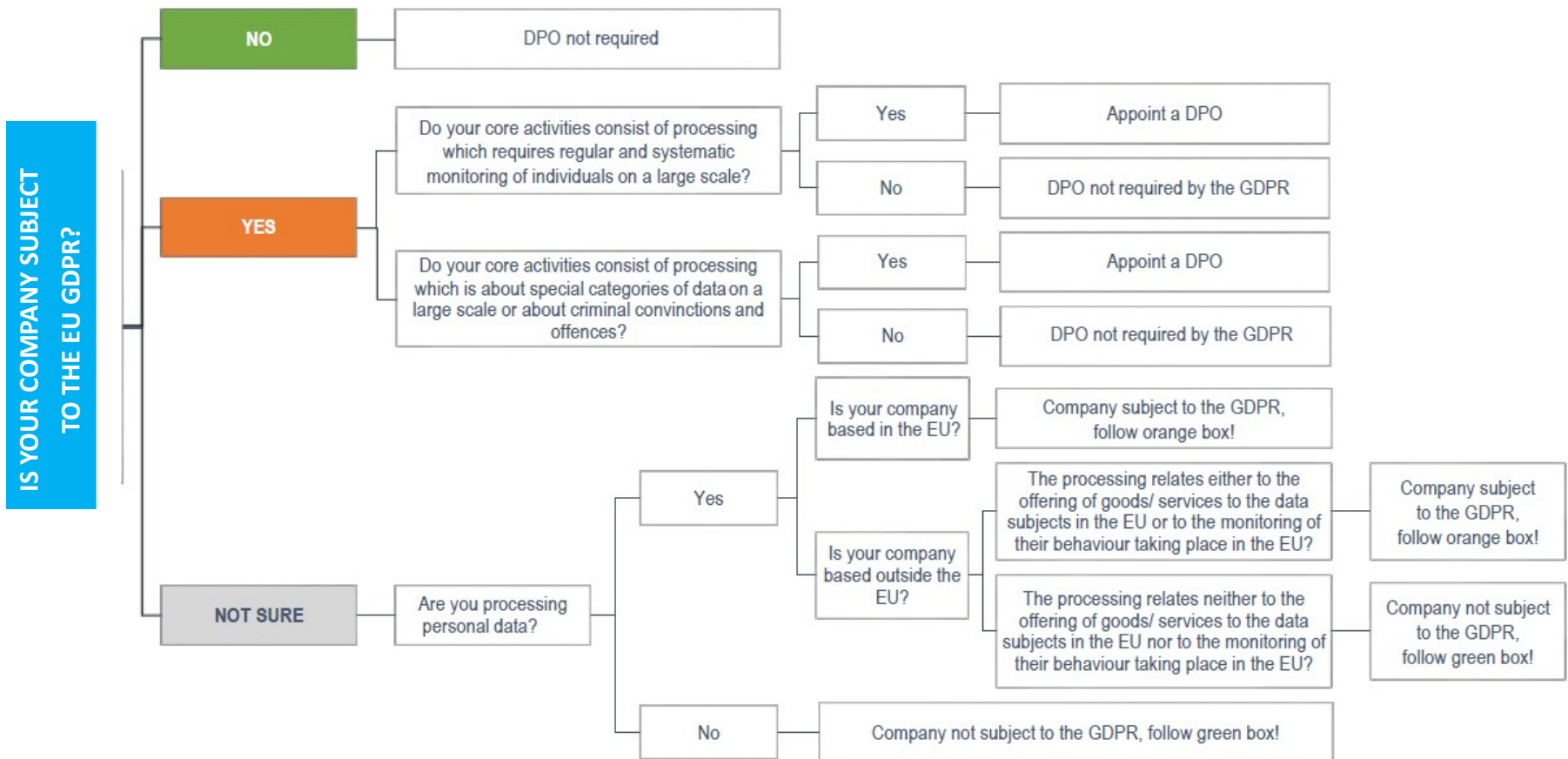
1. Processing is carried out by public authority

2. Required by a national law (eg. Germany)

3. Business with a core activity

- Processing operations require monitoring of personal data at large scale
 - Included hospitals for health data, marketing agency for customer web data, surveillance companies
 - Excluded payroll for a commercial organization, health data by a single doctor
- Processing operations requiring monitoring of sensitive personal data at large scale relating to criminal convictions and offences

Who needs a DPO?




What does a DPO?



- ✎ Foster the data protection culture
- ✎ Guide the GDPR implementation and monitor compliance
- ✎ Make recommendations in meetings where decisions with data protection implications are taken
- ✎ Cooperate and liaison with the supervisory authorities
- ✎ Independence to ensuring compliance
- ✎ Employee or external consultant based on a service contract
- ✎ Expertise in national and European data protection laws
- ✎ Knowledge of the business sector and of the organization of the controller
- ✎ Professional ethics and lack of conflict of interests
- ✎ Groups may designate a single DPO

Group discussion



 **Who can be a DPO? The chief risk officer, the compliance officer, the chief information security officer....**



Core functions of a DPO



- ✎ Implementation of compliance
- ✎ Monitoring compliance
- ✎ Follow up
- ✎ Building awareness
- ✎ Cooperation with DPAs
- ✎ Advice the data controller, data processor and their employees
- ✎ Assist Data Protection Impact Assessment
- ✎ Act as a focal point of contact
- ✎ Assist demonstration of compliance

Independence








Key for assuming the monitoring obligations resting with the Data Protection Authority

- ✎ Through separation of duties (art 38)
 - ✎ Avoid conflicts of interest (no self-monitoring, impartiality, no relatives)
 - ✎ Forbidden to manage IT systems (CISO/CIO) and privacy risks (generally involving board members and HR, compliance, legal and marketing functions)
 - ✎ Lead to a dedicated full time position
 - ✎ It may justify to outsource the role in an independent contractor
- ✎ Direct report to the CEO or highest management level


Independence



Protected employment status

-  Freedom from unfair dismissal (for performing delegated tasks)
-  Appointed for a 2 to 5-years term
 -  (reappointed up to 10 years in total)
-  No penalized in disagreeing with the business
-  Can be dismissed for performance and ethical issues

Separated budget




-  Incl. training, staff, travel, IT solutions, external advise and equipment

Professional qualities of an experienced manager






Requirements



Expert knowledge of data protection law (art 37)

-  Privacy lawyer (but not single skilled)
-  Do not need to be a lawyer to understand one regulation with 99 arts
-  Also: auditor, compliance specialist, IT specialist, non-technical manager





Many non-legal skillset

-  Info security, risk assessment, compliance, business strategy, data governance, change management and public relations
-  High seniority to be a trusted business advisor and leader
-  Formal certifications (by country)
-  Maintain confidentiality
-  Physical location is not relevant, but should be reachable




Tasks (art. 39)



Tips

-  Really understand the organization-specific privacy and security risks
-  Link the risks to the nature, scope, context, & purposes of processing
-  Clearly agree on the title, status, position and tasks
-  No individual liability for non-compliance by the business

Contact point

-  Consult and co-operate with supervisory authorities
-  Notification of breaches
-  Not a whistleblower role! Not a Data Police Officer!

Tasks (art. 39)



- ✎ **Independently**, monitor compliance with the GDPR
 - ✎ Audits against GDPR, internal policies and contracts
 - ✎ Keep the inventory of processing operations
 - ✎ Prioritize controls in a privacy program and monitor compliance
 - ✎ data protection policies, training, data security practices, maintain documentation
 - ✎ Ensure that responsibilities on privacy controls are clear
 - ✎ Supervise the data protection impact assessments and **monitor the action plans**
 - ✎ Handle data subject requests
- ✎ **Strategically**, inform and advise on data protection issues
 - ✎ Attend relevant meetings about data processing (**before** decisions are made)
 - ✎ Train and raise awareness to staff managing personal information
 - ✎ Suggest potential solutions, legal interpretational and implementation changes
 - ✎ Involved in any security breach
 - ✎ Business is not required to follow the DPO's advice

DPO Skills



- 1 Regulations } GDPR
Local national provisions
 - 2 Technical and organizational measures and procedures
 - 3 Data security by design and by default
 - 4 Industry and sector-specific knowledge
 - 5 Experience with the size of the controller or processor
 - 6 Awareness of the sensitivity of the data processed
 - 7 Experience in inspections, consultation and analysis
 - 8 Ability to document processes
 - 9 Ability to work with data subjects' and employees' representation organizations
 - 10
- And get ongoing advanced training!

- ✎ **Communicate the contact details of DPO to**
 - ✎ the supervisory authority
 - ✎ the public for complaints and disputes
- ✎ **External-facing role**
 - ✎ Independent monitor of data protection compliance
 - ✎ Keep the inventory of processing operations

Voluntary



✎ DPOs can be voluntarily appointed in private organizations

✎ When it is not required by the GDPR

✎ Reason: reduce eventual fines

✎ They can be officially communicated to the Supervising Authority

✎ Once registered, the DPO will follow the same requirements as obliged

✎ Alternative, informally allocate responsibility for data privacy compliance to other employee

✎ Tip: do not name the position/role as DPO, but as Data Privacy Officer

✎ Chief of Internal Audit? IT audit/compliance experts?

Relationship with the Board



- ✎ The DPO should directly report to the highest mgmt level (art. 36.2)
- ✎ Reporting line to top management, e.g. CEO, board president
- ✎ Sell data protection as a competitive advantage to the Board
- ✎ Understand issues discussed by the Board
 - ✎ new products, technologies, industry-specific, stakeholders' needs
- ✎ Independence requires a channel to escalate issues to the Board
- ✎ Approval to update policies to add privacy controls
- ✎ Usual reports from the DPO to the Board
 - ✎ operation of the privacy program: key performance indicators, training
 - ✎ risk map: new risks, changes in regulations, ignored recommendations
 - ✎ data breaches: past events, consequences, prevention plans
 - ✎ investments: cost of compliance, future budget, plans

Relationship with the CIO



- ✎ **Historically, the CIO took personal data protection responsibilities**
- ✎ The CIO is a partner for improving the privacy culture
 - ✎ Key: educate the CIO on the new GDPR requirements and best practices to comply with them (what and how)
- ✎ **A good working relationship, but separated**
 - ✎ Clearly identify personal data protection issues to involve the DPO from all other IT tasks
 - ✎ Many shared concerns: confidentiality, security, tools, access controls,...
- ✎ Many remediation actions for GDPR compliance are owned by the CIO
- ✎ The DPO has a consultation (and approving) role
 - ✎ DPIA, privacy by design/default, approve the go-live of apps dealing with personal data

Breakout session/Discussion in groups



- ✎ What are the first three things you would do in your role as the DPO?
- ✎ In what manner, & how often, will you keep the board informed of the activities?
- ✎ What are the ethical responsibilities that you will maintain to ensure confidentiality?
- ✎ How will you maintain your independence while working closely with the organisation?
- ✎ How will you influence the use of DPIAs, privacy seals, and information security standards as a DPO?



Documentation requirements



- ✎ **Policies**
- ✎ **Objectives**
- ✎ **Scope**
- ✎ **Procedures**
- ✎ **Controls**
- ✎ **Risk assessment methodologies**
- ✎ **Risk treatment plan**
- ✎ **Documents protection and control**

Payment Card Industry Data Security Standard



Definition

Information security standard covering payment card and cardholder data
Cardholder data is scoped by GDPR

How it helps GDPR?



Methodology for securing cardholder data
Encryption of critical data
Identify and remediate vulnerabilities (i.e. penetration tests)
Implement strong access control measures
Daily review of security events and logs
Guidance on conducting data protection impact assessments

NIST Guidance



Definition

Frameworks and methods to help organizations to deal with cyber risks
I.e. NIST 800-53 on privacy policy

How it helps GDPR?



How to identify different types of information that are processed, stored, or transmitted
How to assess risks
How to maintain a record of security controls
Develop security architectures to allocate security controls including monitoring communications

Automated decision making



Profiling



fully automated decision-making
(*machine learning*)

ability to make decisions by
technological means without
human involvement

decisions on an
individual cannot be
solely based on
automated processing

unless the individual
gives an explicit
consent

Automated decision making



There are three exemptions when they apply in processing the data:

- is necessary for entering into, or performance of, a contract between the data subject and a data controller;
 - is authorised by a union or member state law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
 - is based on the data subject's explicit consent.
-
- Article 13 states that data subjects have the right to an explanation of the logic involved. I
 - DPR does not forbid profiling. It requires the transparency of all operations, appropriate statistical procedures and accuracy of data.
 - Requires a strong emphasis on the right to opt out that is enforced in all areas where consent is involved, not just profiling.

Exercise



Case

Imagine that you are the DPO of a large advertising company which monitors behaviours of individuals (*profiling*) and collects their personal data (registration information, search activities, browsing history, visited pages, time spent in a website, purchasing habits, location, hobbies, age, sex and) to make customised ad. The company regularly posts the customised ad.

Task

1. What should be your approach and action plan to ensure GDPR compliance.

When the DPO is needed?



If **public authority or body**

(except for courts acting in their capacity)

If **core activities** consists of processing operations...

If required by the **Union or Member State Law**

Possibility of **single DPO for several authorities**

(considering their structure and size)

Requiring regular and systematic monitoring of data subjects on a large scale

Dealing with special categories of data and criminal convictions and offenses

Group of undertaking may appoint a **single DPO**, if accessible

Position of the DPO?



Recruitment base



The DPO shall be designated on the basis of 1) **professional qualities** and 2) **expert knowledge of data protection laws and practice** and the ability to fulfil the tasks

Conjunction



- 1) **Employed** by the data controller or processor
- 2) **Service contract** (independent contractor)

Reporting line



Directly to the highest management level of the data controller or processor

Obligations



- 1) **Keep confidentiality** about the performance of tasks, in accordance with EU and national laws
- 2) Perform duties in an **independent manner**

Tasks of the DPO?



Inform



Advise



Monitor



Contact
point with
the SA



Other tasks

Without creating a
conflict

(DPO as a part time job)

To inform and advise the data controller or processor
and the employees processing personal data
concerning their obligations under the...

GDPR and EU Laws

National Laws

Advise on impact assessment and monitor its
performance

Advise on how to adopt personal data protection
policies

Tasks of the DPO?



To do this...

Inform

Advise

Monitor

Contact
point

The data controller or processor shall **support the DPO** in performing their tasks by

Develop internal policies to demonstrate compliance and **audit** their adoption



Resources to carry out the tasks (budget for a privacy program)



Access to personal data and processing operations (political authority)



Maintain the expertise of the DPO (training)

Develop training and awareness campaigns

Obligation to display contact information



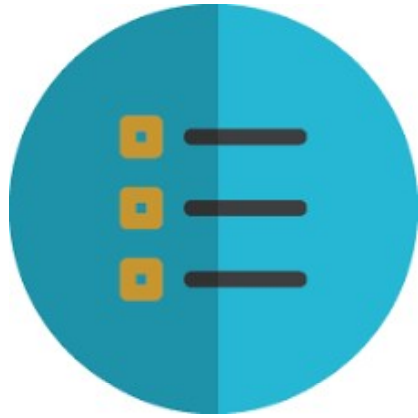
In connection with?	Who?
Personal data collection	DC
Records of processing activities	DC
	DP
Personal data breaches	DP
Prior consultation. High risk	DC
DPO accession	DC/DP

Obligation of other to display DPO



Where?	To whom?	Article?
Information i.c.w. proactive disclosure duty	Data Subject	13/14, § (1), point b
Record of processing activities under Art. 30	SA	30, § (1), point a
		30, § (2), point a
Reporting	DC	33, (3), point b
Consultation	SA	36, § (3), point d
Notifications	SA	37, § (7)
In the publication (Web)	Public	

GDPR




GDPR Compliance Checklist




GDPR Compliance Checklist I/II



Territorial scope

-  identify non-EU group companies that monitor, track or target EU data subjects

Supervisory authority to determine and assert jurisdiction

-  determine the organisation's main establishment/central administration is,
-  where decisions on processing personal data are taken
-  where the main processing activities take place



Data governance and accountability

-  DPO, Design and default, Privacy impact assessments (DPIA), Training
-  identify key stakeholders, demonstrate compliance, consent, reporting lines

Export of personal data

-  identify where personal data is processed within organisation, & third party



Controllers and Processors

-  intra-group, customer or service provider arrangements where a group company is a joint controller
-  intra-group processor agreements, requirements to maintain group liability


GDPR Compliance Checklist II/II




Lawful grounds to process and consent

-  For each type or category of processing, identify and document the grounds for lawful processing & legitimate interests
-  The storage period for the data (required for the fair processing notice)

Fair processing information/notices

-  Best process for fair processing in a clear and intelligible and information machine readable form


Data subject rights

-  Assess how the rights trigger and how they will be exercised in both customer and employee contexts

Big Data, research and automated decision making

-  Link between original and secondary purposes, assess the context and relationship between the data subject and controller

Personal data breach

-  Data breach response and notification procedures to meet 72 hour notification deadline to Supervisory Authority

GDPR



GDPR Action Plan

GDPR Action Plan



- ✎ **Create & sign off an action plan document by the involved manager depending on the information type**
 - ✎ Follow-up on action plans and document implementation measures (IT and non-IT changes)
 - ✎ Monitoring of risk registry
 - ✎ On-going and past due audits
 - ✎ Involving board members, list of project stakeholders, budgets, approval
- ✎ **for detected GDPR risks**
 - ✎ Evidence of monitoring on closing issues
 - ✎ Changes to systems and controls are tested as effective
- ✎ **Supervise the data protection impact assessments and monitor the action plans.**

What you have received?

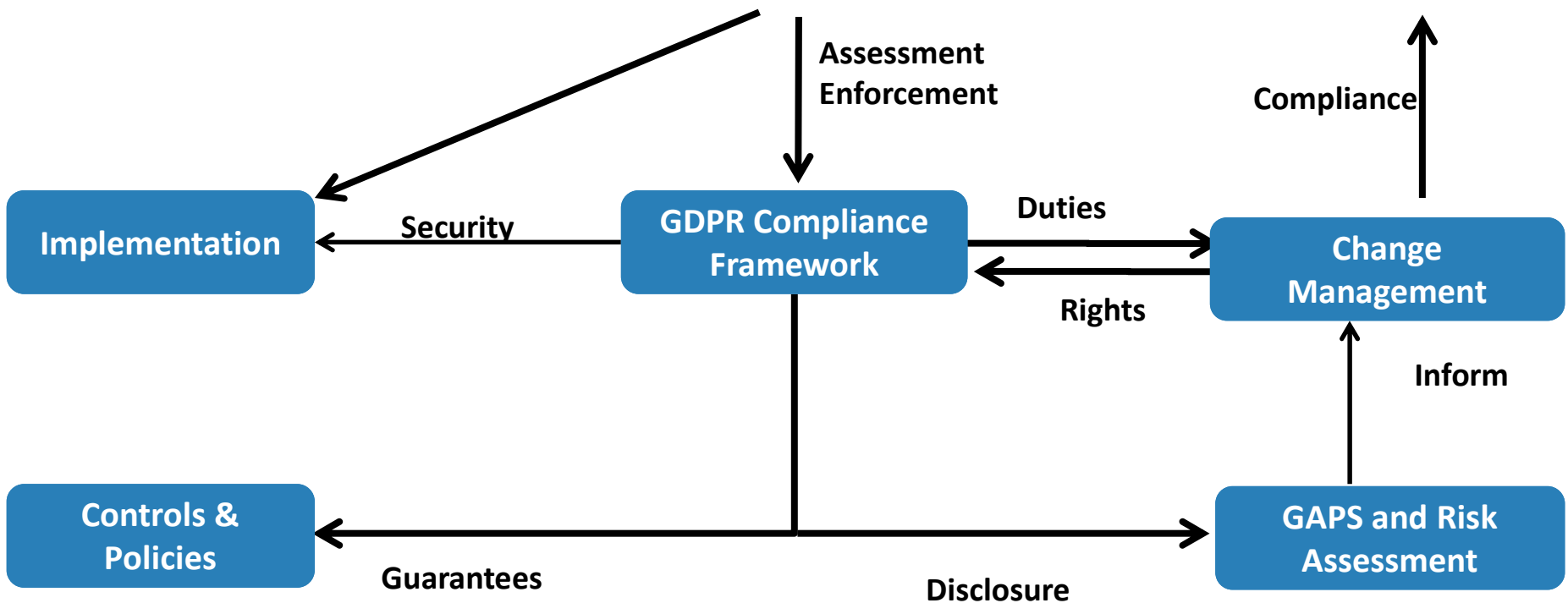


Summary



Project Scope
Territorial and Material

Objectives
bit extra on the top or overhaul of IT platforms, processes & data protection



Useful Data Protection/Privacy/GDPR links



- <https://www.privacyshield.gov/article?id=Privacy-Policy-FAQs-1-5>
 - **Data Protection/Privacy/GDPR Official Text (English, pdf)**
<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>
 - **EU Data Protection/Privacy/GDPR Home Page**
<http://ec.europa.eu/justice/data-protection/>
 - **Working Party 29 Guidance**
http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
 - **Guidelines on “Right to Portability” (pdf)**
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf
 - **Guidelines on Data Protection Officers (pdf)**
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf
 - **Guidelines for identifying a controller or processor’s lead supervisory authority (pdf)**
http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp244_en_40857.pdf
 - UK Information Commissioner’s Office
 - ICO GDPR Home Page
<https://ico.org.uk/for-organisations/data-protection-reform/>
 - **UK ICO – 12 Steps to take now (pdf)**
<https://ico.org.uk/media/1624219/preparing-for-the-Data-Protection/Privacy/GDPR-12-steps.pdf>
 - **EUData Protection/Privacy/GDPR INSTITUTE**
[http://www.euData Protection/Privacy/GDPR.institute/fag/](http://www.euDataProtection/Privacy/GDPR.institute/fag/)
[http://www.euData Protection/Privacy/GDPR.institute/Data-Protection/Privacy/GDPR-thought-leadership/](http://www.euDataProtection/Privacy/GDPR.institute/Data-Protection/Privacy/GDPR-thought-leadership/)
- Full mandate and law:
<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN>



DPO Certification exam



<https://www.eugdpr.institute/gdpr-dpo-exam/>

Presentation as pdf



<https://www.eugdpr.institute/wp-content/uploads/2018/10/fas-slides.pdf>

<https://www.eugdpr.institute/wp-content/uploads/2018/10/dpo-1.pdf>

<https://www.eugdpr.institute/wp-content/uploads/2018/10/dpo-2.pdf>

Copyright notice



The copyright of this work belongs to The GDPR Institute® and Copenhagen Compliance®. None of this presentation, either in part or in whole, in any manner or form, may be copied, reproduced, transmitted, modified or distributed or used by other means without permission from The GDPR Institute®. Carrying out any unauthorized act in relation to this copyright notice may result in both a civil claim for damages and criminal prosecution.

Info@eugdpr.institute

As usual when in doubt always contact your legal advisers. The EUGDPR Institute and Copenhagen Compliance are not licensed to provide legal advice.

The GDPR Institute



www.copenhagencompliance.com



Human Capital Assessment Framework



The GDPR Institute® is the global Governance, Risk Management, Compliance and IT Security (GRC) think tank. As a privately held professional services firm, the mission is the advancement of the corporate ability to govern across the borders, sector, geography, and constituency. The primary aim is to help companies and individuals achieve integrated GRC management that unlocks the Organization ethics, cultures and value by optimising GRC issues to IT-Security & automation thru templates, roadmaps, & frameworks.

The GDPR Institute provides global end-to-end GRC platform, with a comprehensive & proven advisory based on; giving priority to transparency, accountability and oversight issues. Our focus is on GRC Intelligence, Internal Controls, Audit, CSR, Compliance & Policy Management, IT-GRC, Sustainability Management, Bribery Fraud, Corruption (BFC), IT &- Cyber Security Issues

The GDPR Institute® has dedicated resources for consultancy and research in Good Governance, Risk Management and Compliance issues involving corporations, universities and business schools and GRC organizations on four continents.

Disclaimer



- The examples and scenarios in this presentation are for illustration purposes only, and not based on specific examples to be construed as particular advice on any practical legal issues.
- As always, contact your legal counsel for clarification and recommendations on legal issues. Copenhagen Compliance or The EUGDPR Institute is not licensed to provide legal advise.